AO 106 (Rev. 04/10) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the

District of Maine

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

information associated with josefebles22@gmail.com and meylisirueda@gmail.com, that is stored at premises controlled by Google

Case No. 2:16-mj-245-JHR

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment A1 to Affidavit of Special Agent Matthew B. Fasulo, attached

located in the Northern District of California, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B1 to Affidavit of Special Agent Matthew B. Fasulo, attached

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. §§ 1028A, 1029(a)(2), 1029(a)(3), 1029(b)(2)	Aggravated identity theft, access device fraud, possession of fifteen or more unauthorized access devices, conspiracy to commit access device fraud

The application is based on these facts:

Please see the attached Affidavit of Special Agent Matthew B. Fasulo

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of ____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Matthew Fasulo

Applicant's signature

Special Agent Matthew B. Fasulo, USSS

Printed name and title

Sworn to before me and signed in my presence.

Date: 11/28/2016

Judge's signature

City and state: Portland, Maine

John H. Rich III, United States Magistrate Judge

Printed name and title

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT APPLICATIONS

I, Matthew B. Fasulo, being first duly sworn, hereby state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for search warrants for the following:

a. Information associated with the accounts **josefebles22@gmail.com** and **meylisirueda@gmail.com** that is stored at premises controlled by Google, an email provider headquartered at Mountain View, California.

b. Information associated with the account **meylirueda@yahoo.com** that is stored at premises controlled by Yahoo, Inc., an email provider headquartered at Sunnyvale, California.

2. The information to be searched is described in the following paragraphs and in Attachments A1 and A2. This affidavit is made in support of applications for search warrants under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Google and Yahoo to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachments B1 and B2, respectively. Upon receipt of the information described in Section I of Attachments B1 and B2, government-authorized persons will review that information to locate the items described in Section II of Attachments B1 and B2.

3. I am a Special Agent with the United States Secret Service and have been so employed since 1998. I received formal training at the Federal Law Enforcement Training Center in Glynco, Georgia, and the United States Secret Service Academy in Beltsville, Maryland. I am currently assigned to the Portland Resident Office. My current assignment includes investigating

violations of laws against access device fraud, counterfeiting, identity fraud, and computer fraud and abuse. I have received additional training in the forensic analysis of digital storage devices. I was an instructor at the National Computer Forensics Institute and the International Law Enforcement Academies in the investigation of internet-based crimes. Based on my training and experience, I am familiar with the means by which individuals use computers and information networks to commit various crimes.

4. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. §§ 1028A (aggravated identity theft), 1029(a)(2) (access device fraud), 1029(a)(3) (possession of fifteen or more unauthorized access devices) and 1029(b)(2) (conspiracy to commit access device fraud) have been committed by an individual or individuals using the email addresses **josefebles22@gmail.com**, **meylisirueda@gmail.com**, and **meylirueda@yahoo.com**. There is also probable cause to search the information described in Attachments A1 and A2 for evidence of these crimes further described in Attachments B1 and B2.

JURISDICTION

5. This Court has jurisdiction to issue the requested warrants because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that – has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

PROBABLE CAUSE

6. On August 2, 2016, I obtained a criminal complaint against Yaisder Herrera Gargallo, Jose Castillo Febles and Juan Carlos Febles, charging them with conspiracy to conduct illegal transactions with access devices, in violation of 18 U.S.C. § 1029(a)(5) and (b)(2). The affidavit I submitted in support of the criminal complaint is attached as Attachment C and incorporated here.

7. On October 18, 2016, the grand jury for the District of Maine returned an indictment charging the three defendants with conspiracy to commit access device fraud, access device fraud, and possession of fifteen or more unauthorized access devices. On November 15, 2016, the grand jury returned a Superseding Indictment, adding one count of aggravated identity theft against each defendant.

8. As the complaint affidavit at Attachment C indicates, I forensically analyzed the Sony laptop computer seized in connection with the June 18 traffic stop. Among the information I found on the laptop were at least 12 Gmail webmail fragments associated with the email address **josefebles22@gmail.com**, showing travel itinerary information. The fragments referenced upcoming trips to Pittsburgh, PA; Washington, DC; Dulles, VA; Baltimore, MD; SeaTac, WA; and Miami, FL. There were also references to Delta flight receipts for Jose C. Febles and Yaisder Herrera for November 10, 2015:

Delta Air Lines <Delta_	Your Flight Receipt - JOSEC FEBLES 10NOV15
Delta Air Lines <Delta_	Your Flight Receipt - YAISDER HERRERA 10NOV15

Most of these travel-related emails were from travel@priceline.com. Priceline is an internet-based travel agency.

9. This travel information is consistent with other information obtained thus far in the investigation indicating that the three co-defendants had traveled to other parts of the country to engage in similar fraudulent activity. For example, many of the credit and debit card numbers found on the Sony laptop were issued by banks and credit unions in the Seattle, Washington, area. As noted above, among the trips referenced in the email fragments was one to SeaTac, Washington, the location of Seattle-Tacoma International Airport.

10. Also stored in the Gmail fragments for **josefebles22@gmail.com** were nine emails from **meylirueda@yahoo.com** and **meylisirueda@gmail.com** between November 25, 2015, and December 16, 2015. The nine emails are listed below:

Email(s)	Subject	Sent Date/Time - Local Time	Attachments
meylsi rueda <meylirueda@yahoo.com\" name=\"meylsi rueda>	(no subject)	Wed, Nov 25, 2015 at 3:11 PM	None
meylsi rueda <meylirueda@yahoo.com\" name=\"meylsi rueda>	Fw:	Wed, Nov 25, 2015 at 11:38 AM	new.txt, plasticos.txt, trabajo.txt
meylsi rueda <meylirueda@yahoo.com\" name=\"meylsi rueda>	Luna	Wed, Nov 25, 2015 at 8:30 AM	new.txt, guanaja 3 bp.txt, new exxon guanaja.txt
meylsi rueda <meylirueda@yahoo.com\" name=\"meylsi rueda>	Fw:	Wed, Nov 25, 2015 at 10:05 AM	new.txt, plasticos.txt, trabajo.txt
meylsi rueda <meylirueda@yahoo.com\" name=\"meylsi rueda>	Luna	Wed, Nov 25, 2015 at 8:30 AM	new.txt, guanaja 3 bp.txt, new exxon guanaja.txt
meylsi rueda <meylirueda@yahoo.com\" name=\"meylsi rueda>	Fw:	Wed, Nov 25, 2015 at 10:05 AM	new.txt, plasticos.txt, trabajo.txt
meylsi rueda <meylirueda@yahoo.com\" name=\"meylsi rueda>	Luna	Wed, Nov 25, 2015 at 8:30 AM	new.txt, guanaja 3 bp.txt, new exxon guanaja.txt
meylsi rueda <meylsirueda@gmail.com\" name=\"meylsi rueda>	(no subject)	Wed, Dec 16, 2015 at 9:30 PM	seattle nordstrom.txt
meylsi rueda <meylsirueda@gmail.com\" name=\"meylsi rueda>	(no subject)	Wed, Dec 16, 2015 at 9:30 PM	seattle nordstrom.txt

11. All of the nine emails contained references to files that were attached to the email messages. The file names of the attachments matched files found on the Sony laptop that contained credit card data. For example, as reflected on the previous page, multiple emails attached a file named "guanaja 3 bp.txt." I found this file in the Downloads folder of the "lorena" user account on the laptop, and found that it contained Track 1 and Track 2 data for

approximately 95 different credit and debit cards. Date information in the text file suggested that the card numbers had been obtained in early November 2015.

12. Based on these email fragments and the text documents also found on the laptop, it appears that an individual or individuals used the email addresses **meylirueda@yahoo.com** and **meylisirueda@gmail.com** to send stolen credit card information to **josefebles22@gmail.com** in November and December of last year.

13. In addition, one of the emails sent from **meylirueda@yahoo.com** to **josefebles22@gmail.com** contained a reference to equipment used to create fraudulent credit cards. A November 25, 2015 email contained a link to a page on a software website, at which software for a magnetic stripe card reader/writer could be downloaded. In my training and experience, I know that individuals involved in the fraudulent use of skimmed credit and debit card numbers use card writers of this sort to encode stolen card numbers on fraudulent cards. These cards can then be used to purchase merchandise at stores, as was done in the transactions I described in my complaint affidavit at Attachment E.

14. Also as noted in Attachment E, on June 18, 2016, Yaisder Herrera Gargallo identified Meylisi Rueda as his girlfriend, and records from Avis car rental showed that the Jeep in which the three defendants were driving when they were stopped on June 18 had been rented by Meylisi Rueda in Boston on June 14.

15. In my complaint affidavit, I described fraudulent transactions that occurred at Walgreens locations at Marginal Way and Allen Avenue in Portland on June 14 and June 15, respectively. Investigators obtained surveillance footage depicting these transactions. I have reviewed this footage, and based on my comparison of the footage with known photographs of

Yaisder Herrera Gargallo and Meylisi Rueda, I believe that Gargallo and Rueda were the two individuals who conducted the transactions.

16. On September 13, 2016, a preservation request under 18 U.S.C. § 2703(f) was submitted to Google, requesting the preservation of all information associated with **josefebles22@gmail.com** and **meylisirueda@gmail.com**. On September 15, 2016, a similar request was submitted to Yahoo, requesting the preservation of information associated with **meylirueda@yahoo.com**.

17. On September 15, 2016, a subpoena was sent to Google requesting subscriber information associated with **josefebles22@gmail.com** and **meylisirueda@gmail.com**. Google responded to the subpoena on September 26, 2016. The information provided in response to the subpoena showed that the **josefebles22@gmail.com** account was created on September 30, 2013, in the name of "Jose Febles." The information also showed that the **meylisirueda@gmail.com** account was created on June 16, 2014, in the name of "meylisi rueda." The recovery email address associated with the account was **meylirueda@yahoo.com**.

BACKGROUND CONCERNING EMAIL

18. In my training and experience, I have learned that both Google and Yahoo provide a variety of on-line services, including email access, to the public. Google and Yahoo allow subscribers to obtain email accounts at the domain names gmail.com and yahoo.com, respectively, like the email accounts listed in Attachments A1 and A2. Subscribers obtain an account by registering with Google or Yahoo. During the registration process, Google and Yahoo ask subscribers to provide basic personal information. Therefore, the computers of both providers are likely to contain stored electronic communications (including retrieved and un-retrieved email for Google and Yahoo subscribers) and information concerning subscribers and

their use of Google and Yahoo services, such as account access information, email transaction information, and account application information. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

19. In my training and experience, Google and Yahoo subscribers can also store with the provider files in addition to emails, such as address books, contact or buddy lists, calendar data, pictures (other than ones attached to emails), and other files, on servers maintained and/or owned by the provider. In my training and experience, evidence of who was using an email account may be found in address books, contact or buddy lists, email in the account, and attachments to emails, including pictures and files.

20. In my training and experience, email providers generally ask their subscribers to provide certain personal identifying information when registering for an email account. Such information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative email addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users. Based on my training and my experience, I know that even if subscribers insert false information to conceal their identity, this information often provides clues to their identity, location or illicit activities.

21. In my training and experience, email providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (i.e., session) times and durations, the types of service utilized, the status of the account

(including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, email providers often have records of the IP address used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the email account.

22. In my training and experience, in some cases, email account users will communicate directly with an email service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Email providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

23. As explained herein, information stored in connection with an email account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, the information stored in connection with an email account can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

24. For example, email communications, contacts lists, and images sent (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the

account at a relevant time. Further, information maintained by the email provider can show how and when the account was accessed or used. For example, as described below, email providers typically log the IP addresses from which users access the email account along with the time and date. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the email account access and use relating to the crime under investigation. This geographic and timeline information may tend to either inculpate or exculpate the account owner. Additionally, information stored at the user's account may further indicate the geographic location of the account user at a particular time (e.g., location information integrated into an image or video sent via email). Last, stored electronic data may provide relevant insight into the email account owner's state of mind as it relates to the offense under investigation. For example, information in the email account may indicate the owner's motive and intent to commit a crime (e.g., communications relating to the crime), or consciousness of guilt (e.g., deleting communications in an effort to conceal them from law enforcement).

CONCLUSION

25. Based on the forgoing, I request that the Court issue the proposed search warrants. Because the warrants will be served on Google and Yahoo, which will then compile the requested records at a time convenient to them, I submit that reasonable cause exists to permit the execution of the requested warrants at any time in the day or night.

Respectfully submitted,

Matthew B. Fasulo
Special Agent
United States Secret Service

Subscribed and sworn to before me on November 28, 2016.

John H. Rich III
United States Magistrate Judge

ATTACHMENT A1

Property to Be Searched

This warrant applies to information associated with **josefebles22@gmail.com** and **meylisirueda@gmail.com** that is stored at premises owned, maintained, controlled, or operated by Google, a company headquartered in Mountain View, California.

ATTACHMENT A2

Property to Be Searched

This warrant applies to information associated with **meylirueda@yahoo.com** that is stored at premises owned, maintained, controlled, or operated by Yahoo, Inc., a company headquartered in Sunnyvale, California.

ATTACHMENT B1

Particular Things to be Seized

I. Information to be disclosed by Google (the "Provider")

To the extent that the information described in Attachment A1 is within the possession, custody, or control of the Provider, including any emails, records, files, logs, or information that has been deleted but is still available to the Provider, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f) on September 13, 2016, the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A1:

a. The contents of all emails associated with the account, including stored or preserved copies of emails sent to and from the account, draft emails, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email;

b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

c. The types of service utilized;

d. All records or other information stored at any time by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files;

e. All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken.

f. For all information required to be disclosed pursuant to this warrant, the physical location or locations where the information is stored.

The Provider is hereby ordered to disclose the above information to the government within 14 days of the issuance of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes evidence of violations of 18 U.S.C. §§ 1028A(a)(1) (aggravated identity theft), 1029(a)(2) (access device fraud), 1029(a)(3) (possession of fifteen or more unauthorized access devices) and 1029(b)(2) (conspiracy to commit access device fraud), those violations occurring after November 1, 2015, including, for each account or identifier listed on Attachment A1, information pertaining to the following matters:

a. Information regarding access device fraud or identity theft, to include credit or debit card numbers, personal identifying information, names, addresses, account information, usernames, passwords, bank accounts, and a method of payment for the stolen data.

b. Information regarding the use of hardware and/or software to obtain card numbers or create cards using stolen card numbers.

c. Information regarding the use of stolen credit or debit card numbers to purchase merchandise or services.

d. Information regarding travel arrangements or travel itineraries.

e. Evidence indicating how and when the email account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the email account owner;

f. Evidence indicating the email account owner's state of mind as it relates to the crime under investigation;

g. The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s).

h. The identity of the person(s) who communicated with the user ID, including records that help reveal their whereabouts, if the communications related to the offenses under investigation.

ATTACHMENT B2

Particular Things to be Seized

I. Information to be disclosed by Yahoo, Inc. (the "Provider")

To the extent that the information described in Attachment A2 is within the possession, custody, or control of the Provider, including any emails, records, files, logs, or information that has been deleted but is still available to the Provider, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f) on September 15, 2016, the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A2:

a. The contents of all emails associated with the account, including stored or preserved copies of emails sent to and from the account, draft emails, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email;

b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

c. The types of service utilized;

d. All records or other information stored at any time by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files;

e. All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken.

f. For all information required to be disclosed pursuant to this warrant, the physical location or locations where the information is stored.

The Provider is hereby ordered to disclose the above information to the government within 14 days of the issuance of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes evidence of violations of 18 U.S.C. §§ 1028A(a)(1) (aggravated identity theft), 1029(a)(2) (access device fraud), 1029(a)(3) (possession of fifteen or more unauthorized access devices) and 1029(b)(2) (conspiracy to commit access device fraud), those violations occurring after November 1, 2015, including, for each account or identifier listed on Attachment A2, information pertaining to the following matters:

a. Information regarding access device fraud or identity theft, to include credit or debit card numbers, personal identifying information, names, addresses, account information, usernames, passwords, bank accounts, and a method of payment for the stolen data.

b. Information regarding the use of hardware and/or software to obtain card numbers or create cards using stolen card numbers.

c. Information regarding the use of stolen credit or debit card numbers to purchase merchandise or services.

d. Evidence indicating how and when the email account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the email account owner;

e. Evidence indicating the email account owner's state of mind as it relates to the crime under investigation;

f. The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s).

g. The identity of the person(s) who communicated with the user ID, including records that help reveal their whereabouts, if the communications related to the offenses under investigation.